MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2016/2017

TEH3221 – ETHICAL HACKING AND SECURITY ASSESSMENT

(All sections / Groups)

09 MARCH 2017
9.00 a.m – 11.00 a.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 6 pages, excluding the cover page, with 5 questions only.

2. Attempt **ALL** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

Question 1:

Please attempt ALL multiple choice and True/False questions. [12 marks]

1. A person who uses existing computer scripts or code to hack into computers, who lacking the expertise to write their own, usually refer to as a _____.
   a. hacker
   b. script kiddie
   c. penetration monkey
   d. cracker

2. _____ sometimes displays a banner to notify the users of its presence.
   a. Spyware
   b. Adware
   c. Webware
   d. Malware

3. To compile the "`syntax.c`" program in *NIX, you enter _____ command.
   a. gcc –x syntax.c –o syntax.o
   b. gcc –c syntax.c –o syntax.o
   c. gcc –c syntax.pl –o syntax.o
   d. gcc –o syntax.o

4. For a Windows computer to be able to access a *NIX resource, _____ must be enabled on both systems.
   a. NetBIOS
   b. SMB
   c. NetBEUI
   d. CIFS

5. In a(n) _____ flaw, a Web browser might carry out code sent from a Web site.
   a. broken access control
   b. command injection
   c. unvalidated parameters
   d. cross-site scripting

Continued .....

6. In a _____ attack, the attacker has the ciphertext of several messages that were encrypted with the same encryption algorithm but has no access to the plaintext, so he or she must try to figure out the key used to encrypt the data.
   a. chosen-ciphertext
   b. chosen-plaintext
   c. known plaintext
   d. ciphertext-only

7. The most non-effective approach to protect a network from malware being introduced is to conduct structured training of all employees and management.
   a. True
   b. False

8. The HTTP CONNECT method starts a remote application-layer loopback of the request message.
   a. True
   b. False

9. A closed port responds to a SYN scan with an RST packet, so if no packet is received, the best guess is that the port is open.
   a. True
   b. False

10. NTFS was implemented to replace FAT16 and FAT32 because of the difficulty in incorporating security in these file systems.
    a. True
    b. False

11. The MBSA cannot check for user account passwords that have dictionary words in them.
    a. True
    b. False

12. One of the most common JavaScript security vulnerabilities is Cross-Site Scripting (XSS). Cross-Site Scripting vulnerabilities enable attackers to manipulate websites to return malicious scripts to visitors.
    a. True
    b. False

Continued .....

Question 2:

a) Fill in the blanks with the most appropriate application layer service:

i. _____: is an application protocol for distributed, collaborative, hypermedia information systems. It is the foundation of data communication for the World Wide Web; usually associated with port 80

ii. _____: is an application layer protocol that facilitates communication in the form of text. The chat process works on a client/server networking model; usually associated with port 194, 6667 or nearby port numbers.

iii. _____: is a TCP/IP protocol used in sending and receiving e-mail; usually associated with port 25.

iv. _____: is the standard security technology for establishing an encrypted link between a web server and a browser; usually associated with port 443.

v. _____: the central protocol used to interconnect Microsoft Windows machines; usually associated with port 137, 138, and 139.

[5 marks]

b) The session hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because *HTTP* communication uses many different TCP connections, the web server needs a method to recognize every user's connections. Do you think a sniffer can help you to capture the packet? If you managed to obtain the transmission packets, what are the useful components of a TCP header which may aid you in session hijacking? Explain your way to conduct a session hijacking.

[5 marks]

c) Refer to the Trojan profiling below, provide an assumption based on the used ports.

Name:	BlueFire
Aliases:	Backdoor.BlueFire.
Ports:	21. 80, 19191
Files:	Bluefire0.1.zip - Bluefire0.35.zip - Bluefire0.36.zip - Bluefire0.41.zip - Bluefire0.50.zip
Created:	
Requires:	
Actions:	Remote Access / FTP server / Telnet trojan
Registers:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\txtfile\shell\open\command

[2 marks]

Continued .....

Question 3:

a) Reported by CBC News on March 2016, "*Norfolk General Hospital, located in Simcoe, Ont., confirms its website was hacked by cybercriminals. The attack appears to be part of a trend of cybercriminals targeting hospitals, including one on the Ottawa Hospital in March and another in February that hit the Hollywood Presbyterian Medical Center in Los Angeles, which paid a USD17,000 ransom to have its systems restored*".

What is this attack? Explain your answer by providing **THREE [3]** preventive measures.

[6 marks]

b) Reported by SANS on November 2016, "*Firmware on certain Android devices has been found to contain a backdoor that has been used to send personal data, including text messages and call records, to servers in China. The issue affects certain low-cost Android phones manufactured in China. The software appears to have been developed for devices sold on the Chinese market and was inadvertently introduced in other markets*".

Explain what is backdoor. If you found that your devices are affected by backdoor, how to remove it?

[3 marks]

c) The issue of unsecure Internet of Things (IoT) devices, like those used in the Mirai botnet distributed denial-of-service (DDoS) attacks, goes beyond poor password hygiene. There are problems with the way the devices are manufactured, and the ways in which they connect to the Internet. There are currently no incentives for manufacturers or consumers to spring for the cost of added security.
Differentiate DDoS and denial-of service (DoS). Suggest **TWO [2]** preventive measures.

[3 marks]

Continued .....

Question 4:

a) TCP (Transmission Control Protocol) provides reliable, ordered and error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. How does TCP ensure its reliability through "three-way handshake"?

[4 marks]

b) If you want to view the network connections for both incoming and outgoing TCP, routing tables, and a number of network interface, which network utility command you can use? Explain how you use it.

[3 marks]

c) Based on the following scenarios, identify the best Nmap scan type and define the Nmap scan command parameter for each of them.

i. Utilize TCP connection process, the most effective in providing a clear picture of the ports you can and cannot access, but very easy to get detected by the system being scanned.

ii. Utilize TCP connection process, but able to prevent the connection attempt appearing in application logs.

iii. Send a packet with the FIN, URG and PUSH flags set.

iv. List the hosts within the specified range that responded to a ping.

v. When a firewall blocks outgoing ICMP Port Unreachable messages, the port will appear open.

[5 marks]

Continued .....

Question 5:

a) Your Microsoft Word was infected with a macro virus. More surprisingly, you found that it was created by your 10-year-old brother as a practical joke. Do you think he is a good hacker? Is it difficult to create a macro virus? Justify your answer.

[3 marks]

b) "*Trojan horse attack is able to compromise the data protected by IPSec over the Internet.*" Do you think this is possible? Justify your answer.

[5 marks]

c) You are hired as a penetration tester for ABC online banking, and you found that they do not implement any password policy. Please suggest **FOUR [4]** requirements that a good password policy should include.

[4 marks]

End of Page